REMARKS

Claim Status

Applicants thank the Examiner, Ms. Trang T. Daon, for the courtesies extended to applicants' representative during the telephone interview conducted on May 17, 2010, and for her assistance in furthering prosecution on the merits of the instant application. During the telephone interview, the subject matter of independent claims 1 and 12 was discussed. No agreement with respect to patentability of the claims was reached. The following remarks take into account the content of the telephone interview.

Claims 1, 3-10, 12 and 13 are now pending, with claims 1 and 12 being in independent form. No amendments to the claims have been made. Reconsideration of the application is respectfully requested.

Overview of the Office Action

Claims 3 and 4 have been objected to based on a minor informality. Withdrawal of this objection is in order, as explained below.

Claims 1 and 12 stand rejected under 35 U.S.C. §112, second paragraph, as indefinite for failure to particularly point out and claim the subject matter which applicants regard as the invention. Withdrawal of this rejection is also in order, as explained below.

Claims 1, 3-10 and 12-13 stand rejected under 35 U.S.C. §103(a) as unpatentable over "Clustering Intrusion Detection Alarms to Support Root Cause Analysis", IBM Research, Zurich Research Laboratory, ACM Transactions on Information System Security, Vol. 6, No. 4, pgs. 443-474, November 2003 ("*Julisch*") in view of U.S. Patent No. 6,732,153 ("*Jakobson*").

Applicants have carefully considered the Examiner's rejections, and the comments provided in support thereof. For the following reasons, applicants assert that all claims now pending in the present application are patentable over the cited art.

Amendments Addressing Section 112 Issues and Formalities

The Examiner has stated that "Claims 3-4 are depended on canceled claim 2 (i.e., claim 2)". Applicants have amended claims 3 and 4 in a self-explanatory manner. Withdrawal of this objection is deemed to be in order.

The Examiner has stated that in claims 1 and 12, "completing the description of each of said alerts with sets of generalized valued attributes induced by the taxonomic structures" is not clear, to the Examiner, as to how the description of each alert is associated with the sets of generalized attributes.

As explained at paragraphs [0054] to [0056] of U.S. Pub. No. 2007/0150579 (i.e., the published application), "[a] step E3 completes the description of each of the alerts issued by the intrusion detection sensors 11a, 11b, 11c with sets of values induced by the taxonomic structures based on the valued attributes of those initial alerts to form complete alerts. The valued attributes of the alerts produced by the intrusion detection sensors are the most specific of the taxonomies. Accordingly, on receiving a given alert, the alert management system 13 can, for example, complete the description of that alert by recursively recovering from the generalization relationships of the taxonomic structures a set including the more general valued attributes that have not already been included in the description of another alert previously completed".

As further explained at paragraph [0057] of the published application, "the description of a given alert is completed by a process that consists in working back through a given taxonomy

starting from a given valued attribute. If a valued attribute exists already in the description of another alert processed previously, then this process is stopped; if not, it is added, and the process is iterated from this added valued attribute".

In view of the foregoing, applicants contend that claims 1 and 12 properly comply with the requirements of 35 U.SC. §112, second paragraph. Accordingly, withdrawal of this rejection is also deemed to be appropriate.

Patentability of the Independent Claims Under 35 U.S.C. §103(a)

The Examiner (at pg. 4 of the Office Action) acknowledges that *Julisch* does not disclose the completing, storing and consulting steps recited in independent claim 1 and correspondingly recited in independent claim 12. The Examiner has further acknowledged that *Julisch* does not disclose that "each complete alert is saved in the logic file system as a file with a completed description of each complete alert expressed using propositional logic", as additionally recited in independent claim 1 and correspondingly recited in independent claim 12, and cites *Jakobson* for these features.

Applicants respectfully disagree that the combination of *Julisch* and *Jakobson* either teaches or suggests applicants' claimed invention as recited in independent claims 1 and 12.

Jakobson relates to a knowledge-based method of parsing alarms and other event messages generated by active elements of managed networks to enable fault root cause analysis and to generate trouble tickets (see col. 1, lines 18-33). Specifically, *Jakobson* (col. 1, lines 60-63) describes "a universal parsing service that operates over various levels of message classes". Fig. 1 of *Jakobson* depicts a distributed network system 100 including, *inter alia*, a network mediation service 110, an event notification service 170 and a message parsing service

120. *Jakobson* (col. 4, lines 16-42) explains that the message parsing service 120 receives raw messages (i.e., events) from network elements 102a-102c via the network mediation service 110 and the event notification service 170 and produces parsed messages.

Fig. 2 of *Jakobson* depicts an embodiment of the message parsing service 120 of Fig. 1. *Jakobson* (col. 3, lines 30-33) explains that the message parsing service 120 is based on a message parsing knowledge structure called "Message Class Grammar (MCG)" as depicted in Fig. 3. The Examiner asserts that this MCG disclosed in *Jakobson* is directed to an acyclic graph and, hence, constitutes the claimed taxonomic structure as disclosed, for example, at paragraph [0052] of applicants' published application. However, even assuming, *arguendo*, that *Jakobson* teaches applicants' claimed taxonomic structure – which it does not – *Jakobson* fails to teach or suggest "completing the description of each said alerts with sets of generalized valued attributes induced by taxonomic structures based on the valued attributes of the alerts to form complete alerts", as expressly recited in independent claim 1 and correspondingly recited in independent claim 12.

In fact, in contrast to the Examiner's proffered interpretation of the *Jakobson* MCG, the MCG described in *Jakobson* quite simply does not correspond to the taxonomic structures of applicants' claimed invention. The taxonomic structures of independent claims 1 and 12 define the generalization relationships between valued attributes of alerts issued by intrusion detection sensors. In contrast, the MCG of *Jakobson* includes nodes that represent message classes and arcs therebetween that "correspond to class-subclass relations (i.e., parent-children relations) between the message classes". According to *Jakobson*, each message class specifies data and methods needed to parse a particular subpart of a message (see, e.g., col. 6, lines 41-51). Accordingly, *Jakobson* teaches that the MCG merely defines how each subpart of a raw message

is to be processed for the purpose of parsing. *Jakobson* specifically describes the parsing process at col. 7, line 36 to col. 8, line 28.

Moreover, *Jakobson* fails to teach or suggest a step of completing the description of alerts with generalized valued attributes. *Jakobson* merely teaches that "raw" messages having a plurality of subparts are parsed by the message parsing service 120 based on an acyclic graph (i.e., the MCG). Indeed, there is no mention whatsoever in *Jakobson* of the terms "generalization" and/or "generalized". Thus, in the absence of any teaching or suggestion of these or equivalent terms, *Jakobson* necessarily fails to teach or suggest "completing the description of each of said alerts with sets of generalized valued attributes induced by the taxonomic structures based on the valued attributes of said alerts to form complete alerts", as expressly recited in claim 1 and correspondingly recited in claim 12.

Jakobson also fails to teach or suggest the storing step recited in claim 1 and correspondingly recited in claim 12. More specifically, independent claim 1 requires storage of the complete alerts in a logic file system to enable the complete alerts to be consulted, where each complete alert is saved as a file with a completed description of each complete alert using propositional logic. That is, independent claim 1 recites "storing said complete alerts in a logic file system to enable said complete alerts to be consulted" and "wherein each complete alert is saved in the logic file system as a file with a completed description of each complete alert expressed using propositional logic". *Jakobson* fails to teach or suggest this subject matter.

The Examiner asserts that the MCG of *Jakobson* is stored in memory repository 260 (Fig. 2). Applicants disagree. *Jakobson* (col. 7, lines 13-14) teaches that the repository 260 is merely intended to store the MCG itself. *Jakobson* (col. 7, lines 21-23) explains that "[o]nce the MCG is developed and validated, it may be retrieved from repository 260 by Java data engine 250 and

made available to universal parsing procedure 270". *Jakobson* thus merely teaches that an MCG (which the Examiner incorrectly asserts corresponds to a taxonomic structure) can be stored in a repository. At best, *Jakobson* would therefore teach the skilled person to store MCG parsing rules and procedures within a repository.

Moreover, even assuming, *arguendo*, that the "raw messages" of *Jakobson* do constitute applicants' claimed "complete alerts" – which they do not – *Jakobson* nevertheless still fails to teach or suggest the storing step of independent claim 1. In fact, *Jakobson* provides no detailed explanation of how to store "raw" or unprocessed messages. Rather, the messages in the *Jakobson* system are merely passed by the managed networks 102a-102c to an event notification server over a "raw" channel.

Jakobson fails to provide even the slightest hint, teaching or suggestion of whether and/or how a logic file system or propositional logic should be used. *Jakobson* (col. 11, lines 28-33) merely teaches that various expressions retrieved from the "raw" messages and having the same meaning can be translated into "a standard representation". *Jakobson* fails to teach or suggest "storing said complete alerts in a logic file system to enable said complete alerts to be consulted", "wherein each complete alert is saved in the logic file system as a file with a completed description of each complete alert expressed using propositional logic", as expressly recited in independent claim 1 and correspondingly recited in independent claim 12.

It follows, *a fortiori*, that *Jakobson* fails to teach or suggest the consulting step also recited in independent claim 1 and correspondingly recited in claim 12. The Examiner asserts that col. 5, lines 6-28 and col. 8, lines 10-28 of *Jakobson* teach this expressly recited subject matter of claims 1 and 12. Applicants disagree. *Jakobson* (col. 5, lines 6-28) merely describes COBRA-type communication interfaces (104a-104d) that allow the event notification service

170 to communicate with other services (110, 120 etc.). *Jakobson* (col. 8, lines 10-28) describes how the message parsing service 120 uses the MCG to parse each subpart of a "raw" message. However, nothing in these sections of *Jakobson* relates to the consultation of complete alerts as recited in independent claim 1 and correspondingly recited in independent claim 12. The skilled person would have no reason to understand or conclude that any teaching in *Jakobson* provides a logic formula that is used as a request in the manner expressly recited in independent claims 1 and 12.

Jakobson thus fails to cure the deficiencies of *Julisch*, because *Jakobson* fails to provide that which *Julisch* lacks. Consequently, *Julisch* and/or *Jakobson*, whether considered individually or in combination, fail to teach or suggest the express recitations of independent claims 1 and 12.

Reconsideration and withdrawal of the rejection of claims 1 and 12 as unpatentable over the combination of *Julisch* and *Jakobson* under 35 U.S.C. §103 are accordingly deemed to be in order, and early notice to that effect is solicited.

Dependent Claims

In view of the patentability of independent claims 1 and 12 for the reasons presented above, each of dependent claims 3-10 and 13 is respectfully deemed to be patentable therewith over the prior art. Moreover, each of these claims includes features which serve to still further distinguish the claimed invention over the applied art.

Conclusion

Based on all of the above, applicants submit that the present application is now in full and proper condition for allowance. Prompt and favorable action to this effect, and early passage of the application to issue, are once more solicited.

Should the Examiner have any comments, questions, suggestions or objections, the Examiner is respectfully requested to telephone the undersigned to facilitate an early resolution of any outstanding issues.

It is believed that no fees or charges are required at this time in connection with the present application. However, if any fees or charges are required at this time, they may be charged to our Patent and Trademark Office Deposit Account No. 03-2412.

Respectfully submitted,
COHEN PONTANI LIEBERMAN & PAVANE LLP

By /Lance J. Lieberman/
Lance J. Lieberman
Reg. No. 28,437
551 Fifth Avenue, Suite 1210
New York, New York 10176
(212) 687-2770

Dated: May 18, 2010